IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER DIRECTING A PROVIDER OF ELECTRONIC COMMUNICATION SERVICE TO DISCLOSE RECORDS TO THE GOVERNMENT	)	Magistrate's No.: 07-524

GOVERNMENT'S REPLY MEMORANDUM OF LAW
IN SUPPORT OF REQUEST FOR REVIEW

AND NOW comes the United States of America by its attorneys, Mary Beth Buchanan, United States Attorney for the Western District of Pennsylvania, and Paul E. Hull, Assistant United States Attorney for said district, and hereby files this reply to the memoranda of law filed by amici curiae Electronic Frontier Foundation et al. ("EFF"), Susan Freiwald, and the Federal Public Defender. For the reasons set forth below, the government respectfully asks this Court to reverse the Opinion and Order and grant the Application in the instant case.

SUMMARY OF ARGUMENT

At the outset, the Government commends amici EFF and Freiwald for acknowledging essential legal errors in the reasoning of the Opinion and Order below. For example, amici EFF and the Federal Public Defender admit that historical cell-site information is "a record or other information pertaining to a subscriber," and that it therefore falls within the scope of section 2703, contrary to the ruling below. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. ("EFF Mem.") at 6-8; Brief of Amicus Curiae Federal Public Defender ("FPD Mem.") at 3 (amicus "does not agree that [cell-site location information] is excluded from protection under the [Stored Communications Act]").

Similarly, amicus EFF concedes that 47 U.S.C. § 1002 – upon which the Opinion and Order places so much weight – does not even apply to the Government's present application for historical cell-site records. *See* EFF Mem. at 13. And both EFF and the Federal Public Defender acknowledge that the Opinion and Order mistakenly relies upon other, equally inapplicable federal statutes to support its erroneous conclusions. *See* EFF Mem. at 10-12 (discussing 18 U.S.C. § 3117, 47 U.S.C. § 222, and Rule 41); FPD Mem. at 2-3.

Nothwithstanding these crucial concessions, amici put forward two main lines of argument in opposition to the Government's appeal. First, amici claim that historical cell-site records are protected by the Fourth Amendment, and that governmental access to them requires a probable cause order. In addition, amici claim that law enforcement access to such records via a 2703(d) "specific and articulable facts" court order enables "dragnet surveillance," and that a court has discretion to demand a showing of probable cause notwithstanding the express language of the statute. Neither set of claims survives examination, and the Court should therefore reverse the Opinion and Order below and grant the instant Application.

I. THE FOURTH AMENDMENT DOES NOT BAR COMPELLED DISCLOSURE OF HISTORICAL CELL-SITE RECORDS PURSUANT TO A 2703(d) ORDER

Amici argue at length that historical cell-site records enjoy Fourth Amendment protection. Specifically, they assert that such records "reveal[] an individual's location in a private space." EFF Mem. at 18; *see also* Freiwald Mem. at 2 ("CSLI, even if imprecise, will almost always indicate constitutionally-protected information about the inside of a home"). For several reasons, these contentions are wholly without merit.

A. Cell-Site Records Are Too Imprecise To Indicate That A Wireless Phone Is Within a Constitutionally Protected Private Area

To begin with, amici provide no factual support whatsoever for their claims about the specificity of historical cell-site records. They neither rebut nor distinguish the authorities cited by the Government – including three separate FCC reports – establishing that cell-site records cannot identify a phone's location more accurately than a range of a few hundred meters at best.[1] And amici simply ignore the sample records, attached to the Government's opening brief as Exhibit C, illustrating that stored CSLI reveals only the location of the serving tower/face but not the precise location of the phone itself.[2]

Instead, amicus EFF attempts to diminish the importance of these sources – and, it would seem, to draw attention away from its own total failure to present factual information in support of its position – with the aside that "[t]he government quibbles with Magistrate Judge Lenihan's factual findings." EFF Mem. at 22. Even worse, amicus Freiwald speculates that "CSLI will grow only more precise over time," Freiwald Mem. at 2, without offering any support for this claim. The Government respectfully submits that the Court should decide the pending Application on the basis of the facts before it, and not on amici's vague speculation about distant future evolution of the relevant technology.

---

[1] *See* Govt's Mem. at 23-24 (quoting three FCC reports and one federal court opinion).

[2] Amicus Federal Public Defender sows confusion with its discussion (FPD Mem. at 10-11) of mid-call handoffs between cellular towers. Amicus does not establish that such handoffs – which occur as a routine matter literally millions of times a day across the U.S. – involve "triangulation" of the phone's precise location. The Court need not resolve this factual question, however, for one simple reason: regardless of the Government's request, no such purported "call handoff" location records are stored and retained by the carriers, as even a cursory examination of Exhibit C reveals.

B. Historical Cell-Site Records Are Created and Retained By Wireless Carriers in the Ordinary Course of Business, And Are Therefore Not Subject to a Reasonable Expectation of Privacy

In addition, amici offer contradictory assertions about the manner in which wireless carriers acquire and retain historical cell-site records. Amicus EFF correctly concedes that the records at issue in this proceeding are "routinely generated and recorded by the cell phone service provider in the ordinary course of providing communications service to its customer." EFF Mem. at 6; *see also id.* at 30 ("CSLI is ... generated by the provider itself as part of its provision of service. ... The tower information is generated whenever the phone is on. The provider decides what historical tower call records to keep.") In contrast, amicus Freiwald claims, without any support,[3] that wireless carriers keep this information at the direction of law enforcement. *See* Freiwald Mem. at 13.

Given EFF's concession, the Court can and should resolve any Fourth Amendment question under the rule articulated in *United States v. Miller*, 425 U.S. 435 (1976). Just as bank records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession," *id.* at 440, historical cell-site records are the business records – routinely created and retained without government compulsion – of wireless telephone carriers.

In that respect, historical cell-site records are no different from any other transaction records. For instance, records of past credit card transactions will often serve to place a person at a given location at a specific time, yet under established Fourth Amendment law they enjoy no Fourth Amendment protection. The novel contrary rationale urged by amici, taken to its logical conclusion,

[3]The sole basis for this claim is apparently the allegation in the Opinion and Order that carriers retain cell-site records "principally, if not exclusively, in response to Government directive." Bare repetition of this unsupported claim does not make it a fact.

would require the Government to obtain a warrant before seeking such records (or bank ATM records, or even corporate records of employee time and attendance). The Court should decline the invitation to invent a previously unrecognized Fourth Amendment interest in this type of routinely gathered business record, and accordingly grant the Application.

C. Even If Analyzed Under the Supreme Court's Cases Concerning "Tracking Devices," Government Access to Historical Cell-Site Records Is Not A "Search" and Therefore Infringes No Fourth Amendment Interest

As noted in the Government's initial brief and above, cell-site information should be analyzed as a business record of a third party, and not under the Fourth Amendment doctrines relating to tracking devices. Even under the latter line of cases, however, government access to historical cell-site information does not infringe a constitutional privacy interest.

In arguing to the contrary, amici misstate the applicable Fourth Amendment doctrines. For instance, EFF insists that "*Knotts* and *Karo* stand for the proposition that there is a reasonable expectation of privacy in the presence of a person or object in a private place." EFF Mem. at 21; *see also* Freiwald Mem. at 8 (arguing that Fourth Amendment test under *Karo* is whether an object has been "withdrawn from public view"). As described below, amici have fundamentally misread *Karo*.

At issue in *United States v. Karo,* 468 U.S. 705 (1984), is not whether persons or objects in private spaces enjoy generalized and undifferentiated Fourth Amendment protection. Rather, as the Court explains at the outset, the exact question is "whether monitoring of a beeper falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance." *Id.* at 707. In that case, agents had installed a radio transmitter in a can of ether expected to be used in processing cocaine. Without first obtaining a warrant, the agents monitored the signal from the beeper as it moved through a series of residences and multi-unit

storage facilities. *Id.* at 708-09.Where the tracking system enabled the government to locate the can of ether in particular residences, the Supreme Court found that the Fourth Amendment had been infringed. *See id.* at 715 ("The beeper tells the agent a particular article is actually located at a particular time in the private residence .... [L]ater monitoring ... establishes that the article remains on the premises.") (emphasis added).

Conversely, the Court found no Fourth Amendment violation where the beeper disclosed only the general location of the ether. In particular, "the beeper equipment was not sensitive enough to allow agents to learn precisely which locker [in the first storage facility] the ether was in." *Id.* at 708. Instead, the agents learned the can's precise location inside a specific locker only after subpoenaing the storage company for rental records; tracking the beeper to a specific row of lockers; and then using their sense of smell to detect the ether. *Id.* When one of the targets moved the ether, a similar scenario played out again: agents traced the beeper to another self-storage facility, and then – using their noses – located the smell of ether coming from a given locker. *Id.* at 709.

As to these two episodes, the Supreme Court held emphatically that no Fourth Amendment violation occurred:

> [T]he beeper informed the agents only that the ether was somewhere in the warehouse; it did not identify the specific locker in which the ether was located. Monitoring the beeper revealed nothing about the contents of the locker that Horton and Harley had rented and hence was not a search of that locker.

Id. at 720 (emphasis added). In sum, the test under *Karo* is not simply whether a tracked object is inside a private, constitutionally protected pocket, purse, or home. (The can of ether was at the relevant times unquestionably in each of the two lockers, both of which enjoyed a reasonable expectation of privacy. *See id.* n.6.) Rather, *Karo* holds that government use of a tracking device

violates the Fourth Amendment only where the monitoring actually reveals the particular private location in which the tracked object may be found.[4]

The rule in *Karo* conclusively disposes of the Fourth Amendment arguments put forward by amici. As set forth at length in the Government's initial brief, historical cell-site records cannot locate a mobile phone even to within several hundred feet except under optimal conditions. Given that no search occurred in *Karo* when law enforcement tracked the can of ether in real time to a given storage facility or even a specific row of lockers, far less accurate historical cell-site records obtained from a carrier cannot possibly intrude upon a Fourth Amendment privacy interest.[5]

Amici argue unpersuasively that *Karo* bars law enforcement from combining disparate facts (and drawing inferences about location from them) without a warrant. *See* EFF Mem. at 21-23; Freiwald Mem. at 4. But as *Karo* itself makes explicit, the agents in that case were free to use the tracking device to track the beeper to a general area (the storage facility), and then to use a subpoena and their sense of smell to infer the precise location of the can of ether, all without conducting a "search." For the same reasons, law enforcement may obtain historical cell-site records – which do not by themselves disclose the presence of a phone or person within private space – and, by comparing them to other information (such as that derived from visual surveillance), draw additional

---

[4]Amicus Federal Public Defender argues in its brief that the precision (or lack thereof) of tracking technology is irrelevant to the Fourth Amendment analysis. *See* FPD Mem. at 7 n.4. We respectfully suggest that amicus has overlooked *Karo*'s unequivocal and controlling holding.

[5]For comparable reasons, amicus EFF is mistaken that *Kyllo v. United States*, 533 U.S. 27 (2001), alters this result. *Kyllo* holds that law enforcement may not use infra-red thermal imaging devices to peer through walls and discern activity inside a home without a warrant. That rule is entirely consistent with *Karo*, and therefore imposes no restriction on the government's access to historical cell-site records, which are incapable of revealing activity inside a specific private space.

conclusions. Adopting the contrary rule advocated by amici would make it unlawful even to use a pen register without a warrant, since the information obtained thereby can indicate whether the occupant of a house is making calls (and therefore inside). Because amici's arguments produce such absurd results and openly question well-established Supreme Court precedent,[6] this Court should reject amici's position and grant the Application.

II. THE 2703(d) STATUTORY STANDARD PROTECTS AGAINST "DRAGNET SURVEILLANCE," AND A COURT MAY NOT IN ITS DISCRETION DEMAND A HIGHER SHOWING OF PROBABLE CAUSE

Amici EFF and Freiwald attempt to portray governmental access to historical cell-site records as "dragnet surveillance" that can be reined in only by requiring a showing of probable cause. EFF Mem. at 24; *see also* Freiwald Mem. at 9. In fact, this melodramatic claim is rebutted by EFF's full-throated advocacy for the very amendment in 1994 that raised the 2703(d) legal standard to its present level requiring "specific and articulable facts."

According to EFF Executive Director Jerry Berman, appearing on August 11, 1994 before a joint House-Senate Judiciary Committee hearing on the pending legislation,

> the bill contains a number of significant privacy advances, including enhanced protection for the detailed transactional information records generated by on line [sic] information services, email systems, and the Internet.
>
> *1. Expanded protection for transactional records sought by law enforcement*
>
> Chief among these new protections is an enhanced protection for transactional records from indiscriminate law enforcement access. ... Provisions in the bill recognize that this transactional information created by new digital communications systems is extremely sensitive and deserves a high degree of protection from casual

[6] *See, e.g.,* EFF Mem. at 19 (openly questioning the holding of *Knotts*).

> law enforcement access which is currently possible without any independent judicial supervision. ...
>
> In order to gain access to transactional records ... law enforcement will have to prove to a court, by the showing of "specific and articulable facts" that the records requested are relevant to an ongoing criminal investigation. This means that the government may not request volumes of transactional records merely to see what it can find through traffic analysis. Rather, law enforcement will have to prove to a court that it has reason to believe that it will find specific information relevant to an ongoing criminal investigation in the records it requested. ...
>
> Court order protection will make it much more difficult for law enforcement to go on "fishing expeditions" through online transactional records, hoping to find evidence of a crime by accident. ...
>
> The most important change that these new provisions offer is that law enforcement will: (a) have to convince a judge that there is reason to look at a particular set of records, and; (b) have to expend the time and energy necessary to have a United States Attorney or District Attorney actually present a case before a court.

Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services, 1994: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103d Cong., 2d Sess. 160-61 (1994) ("Joint CALEA Hearings") (prepared statement of Jerry J. Berman, Executive Director, Electronic Frontier Foundation) (emphasis added).[7]

One month later, EFF offered identical reassurances to a separate House subcommittee. *See Network Wiretapping Capabilities, 1994: Hearings Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy & Commerce*, 103d Cong., 2d Sess. 122-23 (1994)

[7]A copy of the pertinent excerpts is attached for the Court's convenience as Exhibit A. The full record of the joint hearing is available online at http://www.lexisnexis.com/congcomp/getdoc?HEARING-ID=HRG-1994-SJS-0015 .

("House CALEA Hearings") (prepared statement of Jerry J. Berman, Policy Director, Electronic Frontier Foundation).[8] And after Congress passed the legislation and transmitted it for the President's signature, EFF once again hailed the new 2703(d) standard's robust protection against "indiscriminate access" and "fishing expeditions" by law enforcement. *See EFF Statement on and Analysis of Digital Telephony Act* (Oct. 8, 1994).[9] Given these repeated claims in zealous support of enacting the current 2703(d) legal standard, amicus EFF cannot now plausibly claim that this same standard permits unchecked "dragnet surveillance." (Likewise, amicus Federal Public Defender's hyperbolic invocation of George Orwell's *1984* – FPD Mem. at 14 – simply does not square with the standard of proof and court oversight demanded by section 2703(d).)

More to the point, the instant Application plainly seeks a limited set of records pertaining to a single individual, offering specific and articulable facts to show that subject's participation in a drug trafficking conspiracy (and, accordingly, the relevance and materiality of the requested historical cell-site records). Even amicus EFF concedes – albeit grudgingly – that the present Application does not constitute "dragnet surveillance." *See* EFF Mem. at 24.

Nevertheless, amici argue unconvincingly that ECPA permits a judge to demand probable cause of a 2703(d) applicant, and that denial of the Application was therefore appropriate. Curiously, amici are unable to cite a single case so holding (other than the decision below), nor any supporting discussion in the legislative history, even though the operative language has been present

---

[8]A version of Berman's statement (with minor typographic corrections) is available at http://w2.eff.org/Privacy/Surveillance/CALEA/eff_091394_digtel_berman.testimony . The full record of the House hearing is available online at http://www.lexisnexis.com/congcomp/getdoc?HEARING-ID=HRG-1994-HEC-0049 .

[9]A copy of the EFF statement is available at http://w2.eff.org/Privacy/Surveillance/CALEA/digtel94_passage_statement.eff .

since the enactment of ECPA twenty-two years ago. Further, amici fail to reconcile their position with the statute's structure and history, both of which make clear that 2703(d) orders are a mechanism available to the Government in lieu of obtaining a search warrant. *See* Govt's Mem. at 18-19. The effect of amici's argument is, in short, to read section 2703(d) out of the statute and demand a warrant in its place; because the Fourth Amendment requires no such curative reading, this Court should decline the unwise invitation to nullify section 2703(d).

Here, too, EFF's 1994 declarations in support of raising the 2703(d) standard undercut their present claims. In all three of the documents cited immediately above, EFF's Jerry Berman explicitly represented that "the burden or [sic] proof to be met by the government in such a proceeding [*i.e.,* a 2703(d) application] is lower than required for access to the content of a communication [*i.e.,* probable cause under 2703(a)]." *Joint CALEA Hearings* at 161; *see also House CALEA Hearings* at 123 (verbatim); *EFF Statement on and Analysis of Digital Telephony Act* (verbatim). In short, in its efforts to persuade Congress to raise the 2703(d) standard to its current level – "specific and articulable facts" – EFF publicly and repeatedly acknowledged that 2703(d) applications would not require probable cause. This admission contradicts, and fatally undercuts, EFF's current position that the Government can be required arbitrarily to show probable cause, a claim that in any event finds no support in the body of ECPA case law.

CONCLUSION

For these reasons, the government respectfully submits that this Court should reverse the Opinion and Order below and grant the Application in the instant case.

Respectfully submitted,

MARY BETH BUCHANAN
United States Attorney

s/ Paul E. Hull
PAUL E. HULL
Assistant U.S. Attorney
U.S. Post Office and Courthouse
700 Grant Street
Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 894-7311 (Fax)
paul.hull@usdoj.gov
PA ID No. 35302

SOO C. SONG
Assistant U.S. Attorney
U.S. Post Office and Courthouse
700 Grant Street
Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 644-2645 (Fax)
soo.song@usdoj.gov
DC ID No. 457268

MARK ECKENWILER
Associate Director
Office of Enforcement Operations
Criminal Division

U.S. Department of Justice
John Keeney Building
10th Street and Constitution Avenue NW
Washington, DC 20530

NATHAN JUDISH
Senior Counsel
Computer Crime and Intellectual Property Section
Criminal Division
U.S. Department of Justice
John Keeney Building
10th Street and Constitution Avenue NW
Washington, DC 20530